

CRYPTOLOGIA

Volume 35, Number 1, 2011

| | |
|---|-----|
| Was Herbert O. Yardley a Traitor? | 1 |
| <i>John F. Dooley</i> | |
| An Enigma Replica and its Blueprints | 16 |
| <i>Wolfgang Ertel, Lucia Jans, Walter Herzhauser, and Joachim Fessler</i> | |
| American Dragon | 22 |
| <i>Jim Reeds</i> | |
| Secret Keeping 101—Dr. Janice Martin Benario and the Women's College Connection to ULTRA | 42 |
| <i>Robert Edward Lewand</i> | |
| Instances of Arabic Cryptography in Morocco. | 47 |
| <i>Abdelmalek Azizi and Mostafa Azizi</i> | |
| A Key Escrow-Free Identity-Based Signature Scheme without using Secure Channel | 58 |
| <i>Manik Lal Das</i> | |
| William Dean Wray (1910–1962) the Evolution of a Cryptanalyst | 73 |
| <i>Chris Christensen and David Agard</i> | |
| Review of <i>Cryptography and Network Security: Principles and Practice, Fifth Edition</i> | 97 |
| <i>Chris Christensen</i> | |
| Review of <i>Algebraic Cryptanalysis</i> | 100 |
| <i>Chris Christensen</i> | |
| Review of <i>Understanding Cryptography</i>. | 106 |
| <i>Chris Christensen</i> | |

Volume 35, Number 2, 2011

| | |
|--|-----|
| Letter to the Editor. | 109 |
| The David Kahn Collection at NSA's National Cryptologic Museum. | 110 |
| <i>David H. Hamer</i> | |
| Operational Use and Cryptanalysis of the Kryha Cipher Machine | 114 |
| <i>Philip Marks</i> | |

| | |
|--|------------|
| The Cryptology of Baseball | 156 |
| <i>Wayne Patterson</i> | |
| An Accidental Cryptologist: The Brief Career of Genevieve Young Hitt . . . | 164 |
| <i>Betsy Rohaly Smoot</i> | |
| From the Archives: Breaking OTP Ciphers | 176 |
| <i>Jan Bury</i> | |
| Review of <i>The Secret Life of Bletchley Park: The World War II Codebreaking Centre and the Men and Women Who Were There</i> | 189 |
| <i>Chris Christensen</i> | |
| Review of Bletchley Park Trust Reports by Frank Carter. | 192 |
| <i>Chris Christensen</i> | |
| Review of 'Dilly—The Man Who Broke Enigmas' by Mavis Batey | 196 |
| <i>David H. Hamer</i> | |

Volume 35, Number 3, 2011

| | |
|---|------------|
| Letter to the Editor. | 199 |
| Frank Miller: Inventor of the One-Time Pad | 203 |
| <i>Steven M. Bellovin</i> | |
| Steps Toward Unraveling a Vatican Cipher of the 1930s | 223 |
| <i>Franco P. Preparata</i> | |
| Anonymous Authentication with Spread Revelation. | 235 |
| <i>Jan Hajny and Vaclav Zeman</i> | |
| Summary Report of the State of the Soviet Military Sigint in November 1942 Noticing "ENIGMA" | 247 |
| <i>Zdzisław J. Kapera</i> | |
| Cipher against Ciphers: Jonathan Swift's Latino-Anglicus Satire of Medicine | 257 |
| <i>Paul W. Child</i> | |
| US Navy Cryptologic Mathematicians during World War II | 267 |
| <i>Chris Christensen</i> | |
| Keith Batey and John Herivel: Two Distinguished Bletchley Park Cryptographers | 277 |
| <i>Frank Carter</i> | |
| Review of <i>Inside Room 40: The Codebreakers of World War I</i> by Paul Grannon | 282 |
| <i>Chris Christensen</i> | |

Review of *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* by Richard J. Aldrich. 289
Anthony Glees

**Review of *The Bletchley Park Codebreakers*
by Ralph Erskine and Michael Smith. 293**
Chris Christensen

Volume 35, Number 4, 2011

Operation *Stonka*. An Ultimate Deception Spy Game 297
Jan Bury

**John F. Byrne's Chaocipher Revealed: An Historical and
Technical Appraisal. 328**
Moshe Rubin

Annual Contents Listing